Copy to H.C.S.G.. 4/10.

15 (I)

TOP SECRET "U" TICOM/I-106

FINAL INTERROGATION REPORT

ON THE

NORWAY PARTY (NAA 11)

This report supplements the original interrogation of the party reported in TICOM/I-55, Additional interrogations were conducted with Hptm. SCHMIDT at OBERURSEL and with Wtm. BLOMA, Uffz. EXTER and Uffz. BETHGE at I. C. 95 by Major W. P. BUNDY on the basis of a questionnaire furnished by TICOM .

TICOM

18th September, 1945

No. of pages: 7

Copy No. 20

DISTRIBUTION

British:

1. D.D.3.
2. H.C.G.
3. D.D. (N.S.)
4. D.D. (M.W.)
5. D.D. (A.S.)
6.)
7.) C.C.R.(2)
8. Lt. Col. Leathem
9. Cdr. Tandy
10. Major Morgan

U.S.

11.)
12.) Op-20-G(2) (via Lt.Cdr.Manson)
13. G-2 (via Lt.Col.Hilles)
14.)
15.)
16.) A.S.A. (3) (via Major Seaman)
17. Director, S.I.D. USFET (via Lt.Col.Johnson)
18. Col. Lewis Powell, USSTAF

Ticom

19. Chairman
20.)
21.) S.A.C. (2)
22. Cdr. Bacon
23. Lt. Col. Johnson
24. Major Seaman
25. Lt. Cdr. Manson
26. Major Cowan
27. Lt. Fehl
28.)
29.)
30.)
31.) Ticom Files (4)

Additional

32.)
33.)
34.) Lt. Col. Pritchard (3)
35. Mr. Twinn
36. A.D. (W.T.C.)

1) BALTIC NAVAL CALLSIGNS

BLOME had never dealt with this subject and knew of no records. He believed that the Navy had handled this, but did not know what station.

2) "TW" and "RW" IN GERMAN Y-SERVICE REPORTS.

BLOME, ELTER, and BETHGE did not know these terms in German Reports. As a guess they suggested that they were German for RUFZEICHEN WECHSEL and TAGE WECHSEL. The Russians had a term, "TW", for a table of frequencies for assignment to units, but this had no connection with callsigns. There was also a German term, "RTT", for RUFZEICHEN TEIL TAFELN, the basic table of 100 calls from which the Russians chose the daily callsign.

3) BIGRAMS and TRIGRAMS in ADDRESSES.

BLOME knew of the two used separately, but could not recall any case of the two in conjunction. He suggested that this might accompany something he had seen, namely 3Z code mixed into 2Z PT traffic.

4) MORE THAN ONE BIGRAM in the ADDRESS

They could suggest no single explanation of this. The first group of a series might be the "READ LETTERS" group, and the others letter abbreviations of the addressees. Or the addressee might be multiple, or indicated by a double designation. Addresses to personal names rather than titles were common in all Russian traffic, and this suggested the use of initials.

The vagueness of this answer surprised interrogator who asked if the addresses, being enciphered on the PT table, were not read currently. The answer was that unless the same address was used frequently and some outside hint was given they were usually unable to read the address. They supposed it used values which had special local meanings added to the table.

5) PT TABLES AFTER PT 42

The last known table was PT 43, and they could not reconstruct this. PT 43 came in about 1 1/2 years late, at which rate PT 45 would be along next year.

6) DAILY ENCIPHERMENT OF CALLSIGNS, ADDRESSES, AND PT TABLES

The same 10-digit keys were used for all three up to May 1944. After that a special table was used for callsigns, with a second one for addresses and regular encipherment.

7) LIAISON OF NAA 11 WITH THE FINNS AND FINNISH SIG INT ORGANISATION

SCHMIDT supplied almost all of the information on this.

The main FINNISH unit was the RTK, "Radio Telegraf Kompanie". This was about battalion strength, with one motorised companie and a fixed unit of about 200 men located at SORTAVALA. It was commanded by a Colonel whose name S. could not recall. (The Colonel's brother was also an officer in the unit). RTK had about 70 crypt men, mostly officers. (S. scarcely saw them and could recall no names. Neither could the non-coms). They also had evaluation personnel.

The Finns also had an extensive D/F network, directed by special radio and teletype links from SORTAVALA. This had stations up and down the West coast and on the East of the country.

The Finns worked largely on Army traffic and had no separate unit for Air Force Sig. Int.

The Germans had a Sig. Int. Liaison officer, Oblt. RIEMERSCHMIDT, stationed with RTK at SORTAVALA. The Luftwaffe Liaison Officer, Oblt. VAATZ, was at the main Finnish headquarters at MIKKELI and was concerned with all air technical matters, so that Air Sig. Int. formed only a small part of his work. RIEMERSCHMIDT had a direct radio link to NAA 11. SCHMIDT himself was never in SORTAVALA but small Finnish parties did visit NAA 11 from time to time.

Liaison on all crypt matters was excellent. Results were exchanged every two or three days, and NAA 11 varied its cryptographic priorities to give full attention to any special links required by the Finns, the request coming via RIEMERSCHMIDT. The Finnish crypt personnel were considered outstanding and the exchange was a great benefit to NAA 11. RIEMERSCHMIDT also passed to NAA 11 information and solutions received at SORTAVALA from the German LNA itself, and on one occasion (the captured RZ 1800) this was faster than the direct transmission from LNA to NAA 11. The Finns solved 3Z and 4Z codes extensively, with emphasis on NKWD material. The Finns had no success with 5Z traffic and never captured any copies of these codes so far as S. knew.

Finnish "BETRIERSAUSWERTUNG" (traffic analysis) was rated less highly. It was thought that this was due to the Finnish success with solution. Although they had about 20 men in the sector, they did not work systematically nor were they adept at grasping intelligence from the analysis of small amounts of traffic. Thus NAA 11 was able to give more than they got in this respect.

Technical liaison was also handled by RIEMERSCHMIDT and was far more helpful to RTK than to NAA 11. Finnish equipment was mostly German, with some British and, S. thinks, a few American receivers. The Germans gave the Finns much advice but no physical help. On one occasion they put their own apparatus and men at the disposal of the Finns for operation in a key sector during a Russian offensive, but otherwise there was no pooling or sharing of equipment. Much of the Finnish equipment was pre-1939, as old MARCONI D/F equipment.

/D/F

D/F operations were co-ordinated very closely. NAA 11 had no long distance D/F of its own, and relied heavily on liaison with the Finns and with the Luftwaffe. A liaison observer was stationed with the Finnish stations at MIKKELI, YLENE, KEMI, and ROVANIEMI (this according to SCHMIDT. The non-coms. think KEMI was a German Luftwaffe station, that there was no one at YLENE, and that the observer at MIKKELI was primarily there for other purposes with a German unit, MIKKELI being Finnish headquarters as already noted).

The discussion of D/F led to a long description of the LUFTWAFFE Organization. This was NA Komp. 4 of Reg. 355 (OSLO) commanded by Hptm. TUSCEK. The Komp. covered the whole Russian Air Force. It had three fixed detachments (Staffeln) at key points on the front, namely at LUOSTARI (near MURMANSK), in the vicinity of SALLA, and at LIEKSA, and five mobile detachments. D/F stations were located at PORI, OULU, KEMIJARI, and SVANVIK (near KIRKENES).

The main work of 4/355 was on R/T, and this was so successful that they hardly bothered with rear area code traffic. They specialized in spotting the takeoff of planes from Russian airfields, and were credited with 700 Russian planes. Luftwaffe D/F was also excellent and was furnished directly to NAA 11 when requested.

4/355 left Finland at the same time as NAA 11.

Incidental: RIEMERSCHMIDT escaped at the fall of Finland and became adjutant to Oberst BOETZEL of Gen der N.A. SCHMIDT believed he was captured by American forces..... The Finns used military Enigma on their technical radio links. SCHMIDT thought their keys must be secure, as their crypt personnel were so capable..... The Finnish D/F control net used a system of numbers to indicate known links. Unknown links were described in clear.... NAA 11 never got straight intelligence from the Finns or vice-versa. This was characteristic of the general German-Finnish understanding that LAPLAND was a German area for operations with SOUTH FINLAND allotted to the Finns..... NAA 11 never had an intelligence liaison officer with 20 GEB. A.O.K. until September 1944, when both were on the move, and SCHMIDT had to know the desires and intentions of the Army.

8) The 6000 CARDS

These were simply Russian names used in "Auswertung". The file was build up by NAA 11 from P/L and solved traffic, from captured documents, and from ordinary Russian newspapers and broadcasts.

9) NKWD CODES

The NKWD code referred to in I/55 was the RZ 1800. This was the general NKWD code introduced in about February of 1944 as successor to the RZ 1100. The so-called "White Sea" Code broken by NAA 11 was an older (1942?) general NKWD code which was used in the White Sea area from 1943 to the fall of 1944. At that time the White Sea Command adopted the RZ 1800 itself.

a) RZ 1800 The basic code was an alphabetical 4Z code with 10000 actual values (contrasted with the 2000 of the RZ 1600 and RZ 1100 - according to SCHMIDT. The RZ 1100 had been non-alphabetical).

/Ir

It was used in conjunction with substitution tables which were issued by areas. The code itself was captured in the summer of 1944 on another part of the front and was sent to NAA 11 from ICETZEM via RIEMERSCHMIDT. The table for the Karelian front was recovered by NAA 11 and both code and table were believed to be among the papers turned over to TICOM. (Note: a slight difference in nomenclature cropped up on this subject. SCHMIDT regarded the use of tables as an "encipherment", but EXTER spoke of the code as "unenciphered". EXTER then described an indicator system for tables, so it was apparent there was no basic divergence).

The Indicator System consisted of a single 4Z group. The original order was: 1st digit a dummy (always 0), 2nd digit "SEITE", 3rd digit "EINSTELLUNG", 4th digit "ZEILE". In the main Karelian command net the order was originally "SEITE", dummy, "EINSTELLUNG", and "ZEILE". Both orders were varied from time to time.

In addition to the indicator proper (KENNGRUPPE) there was a DATUMSGRUPPE giving the day, month and year plus the length in groups. The group length was minus the KENNGRUPPE and DATUMSGRUPPE, and also minus the code indicator (HINWEISGRUPPE) which was the next to last group noted. Thus the group length was itself a powerful factor in system identification, as it gave the number of indicator groups, which varied from system to system (see below for another method involving a different number of indicator groups).

The use of RZ 1800 was on the highest levels, Stab to Regt., and Regt. to battalion. No addition was ever used with it. (EXTER was emphatic on this point). The code was still in use in September 1944 when NAA 11 left FINLAND, and in April 1945, while in NORWAY, they had intercepted some traffic which they believed to be in this code.

b) The "White Sea" Code. This was an earlier general NKWD code and was an unsystematic 4Z code with 10,000 values. It was issued from the NKWD headquarters at BELOMORSK to the ARCHANGEL headquarters, the 4th GRENZ SHUTZ ABTEILUNG. It was used from the Abteilung (about regimental size) to the 3 subordinate "KOMMANDANTUREN" (battalion size) and by each of them in turn to 4 or 5 subordinate "GRENZPOSTEN" or "FELDWACHEN", thus serving a total of 12-15 links. The units were spread very thin all along the coast from ONEGA to the KANIN-NOS peninsula, being numbered from east to west.

The code was enciphered by additive strips, issued monthly in groups of 10, with 20 digits on each. Each strip had (a) its number at the top (b) the 20 random digits, and the first 10 repeated below (c) setting numbers 0-9. 4 of these strips were inserted in slots according to a daily-changing order in the key sheet. At any given setting of the four strips, 20 4-digit additive groups were available from top to bottom of the slot-holder. (All terms are those of interrogator).

The settings were determined by taking an arbitary basic-setting group and using this group as the setting of a special indicator table with strips similar to the regular additive strips. This table remained constant When the strips of the indicator table were set at the

/basic

basic setting, they provided 20 4-digit groups which were used successively as settings in the addition table. Thus 400 4-digit groups could be enciphered from a single 4-digit basic setting given in the message indicator.

The basic setting was given in the message by subtracting from prearranged groups in the final enciphered text and inserting the resulting groups at other prearranged points in the message. This was done twice for check purposes, at the head and tail of the message. For example:-

(Message of 50 4 - digit groups)

1001	4738	3212	1428	.....
A	B		C	
8953	5643	2150	194547	
B	C		D	

A is the 'HINWEIS GRUPPE - or code indicator.

B are regular text groups at the prearranged positions

C are KENNGRUPPEN

D is the DATUMSGRUPPE (1 September 1945)

C subtracted from B gives basic setting 3310.

In fact the White Sea Code used, in addition, a simple 10-digit table, changed every 10 days, by which B and C were themselves enciphered before the subtraction was performed. The position of B and C changed monthly with the strips.

The group length (47 in the example) omitted the KENNGRUPPEN and HINWEISGRUPPE (constant for the code).

This White Sea Code was tackled by NAA 11 from April to July 1944, and about 60% of the traffic was solved, almost entirely on the higher links. A different key was used to each KOMMANDANTUR and by them in turn to their subordinate units, making 6 keys in all. Solution included only the relative order of the addition strips, never the basic indicator table. Stereotyped air movement messages on the top links were a main aid to solution, and there were many cases of depth.

EXTER and SCHMIDT knew of no work on any double-addition system.

10) SOLUTION OF C36 at JUTERBOG by OKH

BETHGE was asked about solution work on C36 and BC 38. He could recall no solution of BC 38 and recited entirely on C36. He was engaged in the work only from March to September, 1944, with

/PIETSCH

PIETSCH and DOERING of OKH.